~~TOP SECRET~~ TICOM/I-63

INTERROGATION REPORT ON

ORR HERMANN SCHERSCHMIDT

OF PERS. Z. S., AUSWAERTIGES AMT

The attached document is a report on the interrogation of ORR Hermann SCHERSCHMIDT of Pers. Z.S., Auswaertiges Amt, by Major W.P. Bundy, AUS and Capt. J.K. Lively, AUS at HEIDELBERG on 1st August 1945. SCHERSCHMIDT is a specialist in Turkish and Slavonic code-breaking.

TICOM
11 August 1945

No. of Pages 4

DISTRIBUTION

British
Director
D.D.3 (2)
D.D.4
D.D.(N.S.)
D.D.(M.W.)
D.D.(A.S.)
A.D.(C.C.R.)(2)
Lt. Col. Leathem

U.S.
OP 20-G (2)(via Lt. Pendergrass)
G-2 (via Lt.Col.Hilles)
S.S.A. (2)(via Major Seaman)
Director, S.I.D. USFET
(via Lt. Col. Johnson)

TICOM
Chairman
S.A.C. (2)
Cdr. Bacon
Cdr. McKenzie
Cdr. Tandy
Lt. Col. Johnson
Lt. Col. Lewis Powell
Lt. Cdr. Manson
Major Seaman
Lt. Eachus
Lt. Vance
Capt. Cowan
Lt. Fehl
Ticom Files (2)

Additional
Major Morgan

Interrogation Report on Oberregierungsrat

HERMANN SCHERSCHMIDT

Of Pers. Z.S., Auswaertiges Amt

At Heidelberg
1 August 1945

Interrogators:
Major W.P. Bundy, Sig. C.
Captain J.K.Lively, Sig. C.

1. Circumstances. Scherschmidt was located in the eye clinic of the Heidelberg University Hospital, recovering from a cataract operation. Although weak he was mentally clear and his answers were almost too voluble to permit notes. He was completely cooperative, and his whole attitude was exactly like that of other Pers Z.S. people. He was absolutely scientific in his approach and kept fishing for an exchange of information on the subject, appearing surprised at the ignorance of interrogators. In sum, a complete academic, of about B analytic powers.

2. Personal History. Scherschmidt is somewhat over 50 years old. Was a student in 1914, became involved in crypt in the Army, and settled down in Pers. Z. S. soon after the war to make this his life work. Except for the period March 1943 - September 1944, when personal differences caused him to transfer to straight translation work in the document translation section of the A.A., he was with Pers. Z.S. continuously until his capture at ZSCHEPPLIN on 26 April 1945.

3. Crypt Specialties. Scherschmidt was primarily engaged in the linguistic side of cryptanalysis, working on pure codes after the encipherment was removed. (The Polish diplomatic problem was an exception, as the two parts of the problem were inseparable.) Scherschmidt claims to have learned Turkish, Polish and Bulgarian in addition to a smattering of English, French, Russian, and Spanish. He was engaged entirely in Turkish work from 1934 to 1939, and in Polish from 1939 to the end of 1942. While in document translation in 1943-4 he worked on Bulgarian books (and found it very boring), and after his return he did translation and supervision of book-breaking on Turkish codes.

4. Turkish codes. Scherschmidt was not interrogated in detail on his work in Turkish. He said success was very great throughout. In the period 1934-39 the codes were unsystematic (and in Latin at least partially). In 1944-5 the code on which he worked was systematic, with a cyclic additive, and was broken easily.

5. Polish Systems. Scherschmidt worked entirely on diplomatic traffic and was not familiar with military or agent systems or with any successes achieved on them. He had dabbled in Polish throughout his Pers Z.S. career and early in 1939 he was assigned to the main diplomatic code of the Polish Foreign Office. This had been in force since 1934, and some unsuccessful research had been done in an effort to ascertain the encipherment used. The problem was given a very high priority in 1939 and Scherschmidt had first class assistance. With the aid of a captured specimen of encipherment and a captured description of the indicator system, the first message was read early

in 1940. The oode was reoovered gradually, and in 1941 and 1942 all messages were read, most of them currently. The code went out of use in October 1942 and was replaced by a letter code. Scherschmidt did a little work on this at first but did not come back to the problem later. He said the code was never solved, and he did not know details of the attacks made on it by KUNZE and others.

6. From 1935 to 1942 the Polish Government in Warsaw and later in London used a single unsystematic 4-digit code. The consular services used the diplomatic code of the preceding period. In the diplomatic net a separate pair of encipherment tables was provided for each outstation with one pair for broadcast messages. Scherschmidt remembered traffic to the following points from the Polish Government in LONDON: WASHINGTON (very little), CONSTANTINOPLE, MADRID, MOSCOW, ROME (the VATICAN) and BERN. Scherschmidt could not recall the contents of any of this traffic except that he did recall much talk on the MOSCOW link of negotiations between SIKORSKI and STALIN at one period. Scherschmidt remarked that the German White Paper on Poland included no traffic broken by his section; he was told that its materials were captured.

7. Encipherment method. Encipherment tables, used in pairs, contained 100 4-digit groups, 10 x 10. The first ten letters of a particular line of a page in an ordinary book were used to form a transposition key, thus:

Word - O R J E N T A C J A

Key - 8 9 5 4 7 0 1 3 6 2

This key was written horizontally and vertically. The first group of the additive was 01 in Table A, the second was 01 in Table B, the third was 02 in Table A, the fourth 02 in Table B, and so on, using the two tables alternatively until all 200 groups were used. Scherschmidt stated that the groups were then used in reverse key order so that it was possible to get 400 groups from the same ten-letter key. At the same time he insisted that the system did not produce depths. As a simple reversal would produce a reversed depth that could be traced easily, this pair of statements puzzled interrogators. Efforts to clarify the point led only to confusion, which was not aided by Scherschmidt's being unable to read at more than 4 inches distance from the paper even with his good eye. Two explanations are suggested: first, that a second element was used to scramble the order in the second 200 groups; second, and more likely, that the depths, in reversed form, existed all the time but were not guessed by the Germans until they captured the specimen of encipherment. (They would not, of course, appear in text comparisons of enciphered identical code text.)

8. Indicator System. Two 5-figure groups began each message. Scherschmidt did not know the meaning of the 1st digit. 2-4 gave the page of the prearranged book, 5-6 gave the line, 7 gave the "code" indicator (Scherschmidt could not say why this was necessary; he may have meant it was a Table indicator, though this again woulo only be necessary to separate the broadcast from the outstation tables), 8-10 gave the serial number of the message. The page and line indicators were themselves enciphered by a system which did not change and which was captured. However, they never found the books used, so this would only have helped to confirm identical keys. (Scherschmidt could recall no case of this.)

9. Solution Methods. Scherschmidt said that no machinery was used in the solution. The captured specimen of encipherment was stated to be crucial. Presumably it enabled tables of differences to be built up, and solution proceeded from there. All the work was done by hand, and after the initial entry the section was increased in numbers to cope with the mechanical work involved. Message solution was 100% in 1941 and 1942, although the code, being unsystematic, was not reconstructed completely.